

Type stat up, answer arguments

REMARKS

Claims 1-15 are pending in this application (claims 16-30 were previously subjected to an election requirement and withdrawn, then canceled in connection with a Request for Continued Examination). Claims 1-15 stand rejected. In response to the above-identified Office Action, Applicants do not amend or cancel any claims, and do not add any new claims. Reconsideration in light of the following remarks is respectfully requested.

I. Claims Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 1-8 under 35 U.S.C. § 103(a) as unpatentable over *Distributed Systems, Concepts and Design* by Coulouris *et al.* ("Coulouris") in view of *Operating System Concepts*, 5th ed. by Silberschatz ("Silberschatz"), and further in view of U.S. Patent No. 6,098,133 to Summers *et al.* ("Summers").

Claim 1 recites a method comprising several operations, including restricting access to an isolated area of memory to bus cycles performed in an isolated execution mode. The reference relied upon to establish this portion of the claimed method teaches something quite different, so even leaving aside questions about whether the references properly may be combined, Applicants respectfully submit that the claim is not obvious in view of the references.

Summers describes a system to control access from a circuit board or [computer system expansion] card to a peripheral bus in a computer system. Figure 1 shows clearly where the system fits physically: it is an adapter 10 between a motherboard 13 and expansion card 14. Each card that is to be isolated is plugged into an adapter, and when the card is not authorized to access data on the bus, its data lines are effectively disconnected by bus transceivers in the adapter (see col. 3, line 54 through col. 4, line 8).

This is different from the claimed method in several important respects. First, the claim requires that access to an isolated area of *memory* be restricted. Memory is typically not attached to an interface bus like that shown in *Summers* (instead, it is usually accessed through a memory controller that coordinates interactions from the

Type P
Arguments.

Z *Am-Ints*

processor(s) and peripherals). *Summers* does not teach or suggest interposing his isolating bus transceivers between a memory and a data bus, nor would such interposition be likely to work. *Summers* is directed at isolating insecure or untrusted peripheral devices temporarily when sensitive data is being placed on a data bus. System memory is used by processors and all peripherals, trusted or untrusted, and the mix of transactions that involve the memory (e.g. instruction fetches, processor access to data, and peripheral-to-memory DMA cycles) cannot easily be separated into "secure" and "insecure" for isolation purposes. In fact, even if a memory could be isolated and "secure" memory cycles identified, *Summers* could not prevent an untrusted peripheral from viewing the secure data by isolating the memory because the secure peripheral would still need access to the memory – it is the untrusted peripheral that must be isolated, which is why *Summers*'s apparatus is located where it is.

Second, claim 1 requires that two page table maps be maintained, and that the use of one or the other page table be correlated with a normal or isolated execution mode. Even assuming (solely for the sake of argument) that *Summers*'s apparatus could be adapted to isolate a memory, there is no connection between the page tables the Examiner alleges are in *Silberschatz* and *Summers*'s control of the isolating bus transceivers. The final reference, *Coulouris*, provides a more general description of threads, shared memory, and so on. It is not relied upon for any teaching or suggestion concerning the bus cycles to access memory, and Applicants have not located any such material in the portions of *Coulouris* that the Examiner has provided. Thus, *Coulouris* does not remedy the deficiencies noted above.

For at least the foregoing reasons, Applicants respectfully submit that claim 1 is patentable over the references of record, and ask that the Examiner withdraw the current rejection.

Claims 2-8 depend directly or indirectly upon claim 1, and are believed to be patentable for at least the reasons discussed in support of their base claim. Applicants respectfully request that the rejections of these claims be withdrawn as well.

The Examiner rejected claims 9-15 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,615,263 by Takahashi ("*Takahashi*") in view of *Summers* (*supra*). For

reasons similar to those discussed above, Applicants believe these rejections are also inadequately supported.

Claim 9 recites an apparatus comprising several parts, including an isolated execution circuit to generate isolated access bus cycles. *Summers* does teach a circuit to isolate a peripheral card from the rest of a system, but the circuit does not generate bus cycles. Instead, it controls or limits the propagation of data when some other device generates bus cycles. Furthermore, the bus cycles of the other device are not distinguishable based on whether a peripheral card is isolated – in other words, there is no “isolated access bus cycle” that is different from a non-isolated access bus cycle. *Takahashi*, the primary reference, describes a dual mode processor with a secure mode, but also lacks any teaching or suggestion of an isolated execution circuit to generate isolated access bus cycles. For at least these reasons, Applicants submit that claim 9 is patentably different from the references of record, and respectfully request that the Examiner withdraw this rejection.

3rd
Rejection

Regarding claims 10 and 11, those claims depend upon claim 9 and are believed to be patentable for at least the reasons mentioned above. Applicants ask that the rejections of these claims be withdrawn.

Claim 12 recites a platform comprising several parts, including an isolated execution circuit to generate isolated access bus cycles if a processor is executing in an isolated execution mode. This claim stands rejected over the same combination of references discussed in relation to claim 9, and the isolated execution circuit claimed here is similar to the one shown to be distinct from the references in earlier paragraphs. For at least those reasons, Applicants believe claim 12 is also allowable over the references, and ask that this rejection be withdrawn.

Claims 13-15 depend directly or indirectly upon claim 12, and are patentable for at least the reasons discussed above. The Examiner is respectfully requested to withdraw these rejections also.

The Examiner also rejected claims 9-15 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,729,760 by Poisner (“*Poisner*”) in view of *Summers* (*supra*). However, as the Examiner concedes, *Poisner* lacks the isolated execution circuit of independent claims 9 and 12, and as argued above, *Summers*’s apparatus does not

teach or suggest the missing material. Therefore, even assuming (again, solely for the sake of argument) that *Poisner* does disclose all that is attributed to it, and that *Poisner* and *Summers* can be combined, the references of record fail to teach, suggest, or render obvious Applicants' claimed material. Dependent claims 10, 11 and 13-15 have at least the patentable novelty of their base claims, and so all of claims 9-15 are believed to be patentable over the references of record. Applicants respectfully request that the Examiner withdraw these rejections.